Governor's Office for Technology

Security Awareness Newsletter

Published by the GOT Division of Security Services

April 2004 **Volume II, Issue 2**

Inside this issue:

This Issue's Security Tip

Keeping Data Safe in Your Work Area

—Don't leave confidential/sensitive documents on your desk. When not in use, store them in a secure place such as a locked file cabinet.
—Lock your workstation when you are away. Press Ctrl+Alt+Del and select Lock Computer/ Workstation.
—Do not dispose of documents containing confidential or sensitive information in trashcans or recycle bins. Shred or burn the documents if possible.
—Turn off your workstation before leaving for the day.

Internet and Email Acceptable Use Policy

"Do not expect privacy when using the Commonwealth's Internet and email services."

As the Internet and electronic mail have become indispensable business tools, many business and government entities have implemented guidelines outlining the appropriate use of these resources by employees.

To ensure that the Commonwealth's technology resources are not misused or abused, the Internet and Email Acceptable Use Policy (CIO-060) was developed. The policy makes clear to employees that while the State promotes the use of the Internet and email for business purposes, it does not condone the use of these tools for excessive personal use or private business activities.

Below are a few pointers for using the Commonwealth's electronic resources responsibly:

— **Do not** expect privacy when using the Commonwealth's Internet and email services.
— **Do not** state anything in an email that you would not put in a typed and signed letter. Keep in mind that email may be considered a public record and can be made available for review upon request.
— **Do** abide by the generally accepted rules of network and email etiquette.
— **Do** encrypt email containing sensitive or confidential information. (The Commonwealth has selected Entrust products for its encryption needs. For more information on encryption services provided by GOT, contact the GOT Email Team.)
— **Do not** send or forward chain letters or any offensive materials, statements, and/or images.
— **Do not** use the Internet for browsing non-business topics.
— **Do not** use instant messaging or chat software such as ICQ, IRC, or AOL Instant Messenger.
— **Do not** intentionally disrupt the network or users.

The use of the Commonwealth's electronic resources should be viewed as a privilege. By abiding by the acceptable use policy, we not only conserve the state's electronic resources for critical business operations, but reduce the risk of expensive/damaging litigation arising from an employee's misuse of these resources.

A Few Reasons Why an Acceptable Use Policy Makes Sense

—Lost productivity. An employee making $50,000 a year who spends 15 minutes a day answering personal email can cost the Commonwealth $1,600 annually.
—Wasting bandwidth. Use of the web to surf non-business related sites can tie up network resources, negatively affecting the performance of legitimate business applications.
—Legal action. The viewing and distribution of pornography and other offensive materials can expose the Commonwealth to sexual harassment liability.

Did You Know . . .
According to a survey conducted by Gartner, 30 percent of employees' time spent reviewing email is wasted on unproductive email such as chain letters and jokes.

What to Do If You Have Been Hacked

There are numerous ways to secure networks and computer systems. Intrusion Detection Systems (IDS), network firewalls, personal desktop firewalls, and anti-virus software all offer varying levels of protection. The best practice is to use a "defense in depth" strategy or a variety of protection methods to secure a device or network infrastructure. While the servers owned/managed by GOT are protected by a variety of security solutions, intruders have been known to penetrate the most secure systems. With that said, it is always a good idea to be prepared for the worst and become familiar with the appropriate actions to take in the event of a compromise.

Monitoring Systems

Administrators should be familiar with the programs and applications that are running on their systems. This is necessary in order to identify any applications that may have been installed by malicious code or an intruder. In addition, all systems should be monitored for irregular activity. This includes investigating system error reports, reviewing system performance statistics, and monitoring process activity. While system monitoring can be a complex undertaking, the CERT Coordination Center has an in-depth article on this subject that can help administrators gain a better understanding of the task.

Reviewing Event Logs

Reviewing system event logs on a periodic basis is the best way to monitor for intruders. If it is not realistic to manually review logs, Microsoft has a tool called Operation Manager that can provide automatic notification in the event of suspicious activity.

Log files are also very helpful after an intrusion to gain valuable information on how the attacker gained access. Not only do the logs contain useful data on system events, the lack of information may also indicate an intrusion since an attacker will often edit log entries or manipulate the system to prevent the recording of events. It should be noted that accessing the logs on a compromised system may destroy evidence. Therefore, if you believe you have been hacked, it is advised that an investigation be conducted as soon as possible to avoid destroying vital evidence.

Reporting the Compromise

Once it is determined that a security breach has occurred, upper management should be apprised of the situation. The incident should also be reported to GOT by completing a Security Incident Reporting Form (GOT-F012) and submitting it to DSS. The report should include as much information as possible as to why you believe a compromise has occurred, thoroughly detailing any suspicious activity uncovered. DSS Security Engineers will investigate the incident and perform a security audit of the system, if necessary, to determine the extent and severity of the compromise.

Preserving Evidence

If possible, DSS advises that a compromised system be disconnected from the network and that the system administrator be contacted immediately for further instruction. It is recommended that the machine be left up and running until it can be examined. If the machine must be powered down, it should not be shut off via the normal shut down procedures in order to preserve possible evidence that may be stored in the system's cache memory. If the machine is powered down via the normal shut down procedures, the operating system will clear all cache and possibly vital evidence that can be beneficial to the investigation.

Conducting a Security Review

All security accounts on the compromised system and on all of the connected systems should be reviewed. This includes both the local machine accounts and the network accounts (NDS or Active Directory). Any suspicious accounts such as disabled accounts that were recently reactivated should be thoroughly reviewed. Group memberships should also be evaluated to identify if new users have been given more group memberships or more privileges than they should have. The administrators group should be carefully scrutinized since it gives users increased access rights. The system's access control lists (ACLs) should also be reviewed. *Continued on page 3.*

Continued from page 2.

ACLs define the permissions that users, groups, devices, or processes have for accessing it. Tools such as SomarSoft provide a way to capture ACLs in an easily readable format. Entries that appear to give more access than is appropriate should be thoroughly evaluated.

Preparing Compromised Systems for Redeployment

Before redeployment, the system should be examined to determine the reason for the compromise. In addition, adequate processes and procedures should be implemented to protect the system from future intrusion, such as the regular application of security and virus definition updates, confirming the correct configuration for the anti-virus software, enabling appropriate audit logs, and disabling unneeded services.

It is recommended that compromised systems be rebuilt or restored from a backup which was made before the breach occurred. All security patches should be applied to the system before reconnecting it to the network, and the system should be thoroughly scanned for malicious code such as Trojan horse programs that may have been installed during the compromise. The system should also be monitored as it makes connections through the firewall to verify each connection it makes is valid. Since it may not be possible to totally 'hacker-proof' our systems, preparing and planning for the worst before an actual intrusion occurs is the best plan of action. Developing procedures for staff to follow in the event of an attack will increase the organization's ability to act quickly and reduce or even prevent damage.

Detecting Spyware

Whatis.com defines Spyware as "any technology that aids in gathering information about a person or organization without their knowledge." Spyware can include hardware devices such as keyloggers that are secretly placed on the cable between the keyboard and the computer to record keystrokes, or it can be programming code that is concealed in software or cookies and covertly collects user data. Users often unknowingly download Spyware in seemingly innocent freeware/shareware products such as peer-to-peer file sharing programs. Spyware can also be distributed like viruses with users opening apparently benign executable files and unleashing the code. Listed below are some signs of Spyware that you should be on the lookout for:

— The homepage of your browser changes without your intervention. You change it, but it changes back again.
— Your computer displays popup messages when your browser is not running or when not connected to the Internet.
— You get popup messages that address you by name.
— A search toolbar or other browser toolbar appears that you did not install and after removing it, it returns.
— The send/receive lights on your broadband or dialup modem blinks wildly as if you're downloading a file from the Internet when you are not.
— Your system is running slower than usual. To check on your system's performance, open the Task Manager (press CTRL, ALT, DEL and select TASK MANAGER) and select the Processes tab. If you see unfamiliar processes taking up nearly100 percent of the CPU usage, then you likely have Spyware on your machine.
— A new item appears in your Favorites list without you putting it there. You remove it but it returns.

At this time, the Commonwealth does not have an approved Enterprise standard to detect and remove Spyware; however, if you suspect your workstation may contain Spyware, it is recommended that you contact your network administrator for further assistance.

Word to the Wise . . .

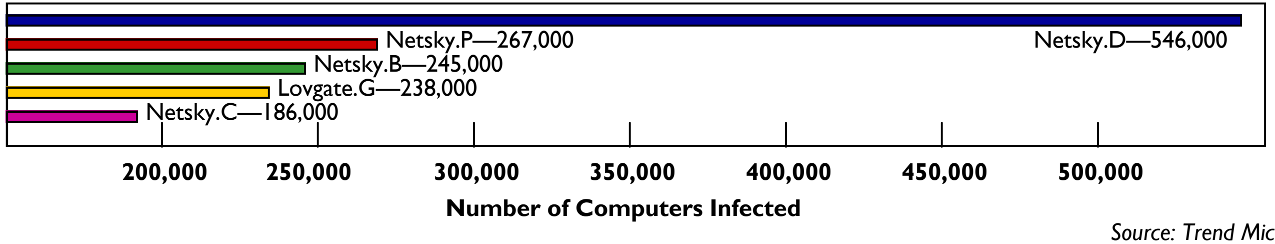
SpyBan, a supposed anti-spyware program, has been accused of being an actual source of spyware. SpyBan is freeware that claims to protect users against spyware; however, it installs a program called Look2Me, which collects information on websites that you visit and sends the data to a server that generates advertisements to be sent to your computer. Another reason not to install anything on your computer that does not originate from a reputable source.

10 Rules for Virus Protection

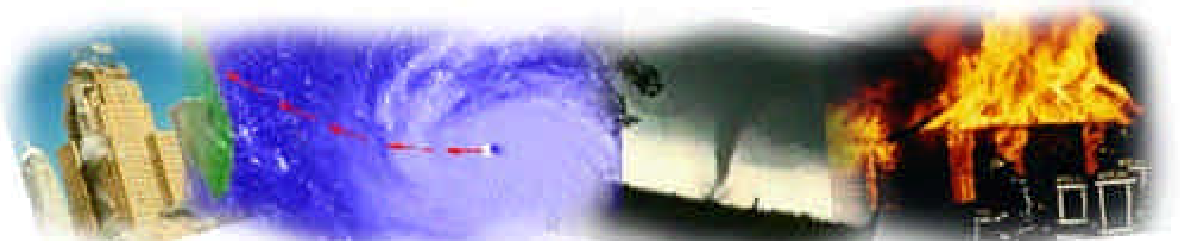
1. **Keep your virus protection software up-to-date.** Virus definition files (McAfee refers to these files as DATs) and engine updates should be applied as soon as they are released by the software manufacturer. Virus protection software will not be an effective deterrent if the latest virus is allowed to infect your system because you failed to keep the virus definition files current. The latest McAfee DATs are available for licensed users on the GOT Security website. (GOT's workstations are configured to update virus definition files automatically on a daily basis.)
2. **Never open an attachment that you aren't expecting.** Most malicious code is spread by opening infected email attachments. Even though the attachment may come from someone you know, many viruses infect unprotected systems and send emails to those that are in the system's Outlook address listing, making it appear that the attachment was legitimately sent.
3. **Perform regular backups of your data.** It is always a good idea to make regular backups of your system and/or important files. If you do happen to get infected with a virus that corrupts your data, your files can be quickly restored.
4. **Reformat if possible.** While it may not always be practical to reformat an infected computer, a low-level format of the hard drive is usually the best course of action to effectively remove malicious code, especially Trojans. The system should be restored from the last uninfected backup.
5. **Keep security patches up-to-date.** For Microsoft users, newer versions of Windows have a *Windows Update* function that makes it easier for you to keep your system patched with the latest security updates. GOT also has a Security Alerts webpage that lists the most current hardware and software vulnerabilities, as well as malicious code threats.
6. **Use a personal firewall**. A personal firewall such as ISS's BlackICE used in conjunction with virus protection software greatly increases your system's security. Click here for a list of approved personal firewall products.
7. **Do not ignore the signs of virus infection.** If you notice any signs of virus infection such as your workstation running sluggish, unexplained error messages, etc. make sure your virus protection software is updated with the latest virus definition files and then scan your system. If you do find a virus, report it immediately to your network administrator and GOT by completing a GOT-F012 Security Incident Reporting Form.
8. **Do not pass on hoax information.** If you receive a virus warning from a friend or family member, don't circulate it unless you can verify that it is legitimate. Some virus warnings are actually hoaxes that can harm your system if you follow their instructions to delete certain system files. If you are unsure of a virus warning, research the virus on McAfee's or Symantec's virus websites. It is also a good idea to sign up for the free virus alert mailing lists that many of the virus protection vendors make available. There are also several helpful sites that provide information on hoaxes:
   Hoaxbusters
   Symantec's Hoax Page
   McAfee's Virus Hoax Page
9. **Be wary of movie, sound, and game files.** These files can also contain malicious code such as viruses, Trojans or spyware.
10. **Don't share your hard drive.** Disable file sharing on your hard drive. If you do need to provide some file and print sharing, use a password and only give the minimum access necessary.

This information was adapted from an article written by Kenneth L. Bechtel, II of Team Anti-Virus.

Current Statistics on the Top Malicious Code Infections During the Past 30 Days



Source: Trend Micro



Disaster Recovery Testing

The Governor's Office for Technology and participating agencies began testing their disaster recovery plans in March. The first phase of testing involved restoring thirty-three (33) mainframe applications at the hotsite, in addition to recovering the mainframe itself. The exercise was a complete success and fully demonstrated the Commonwealth's ability to resume normal business operations within a 48-hour timeframe after declaration of a disaster. Agencies and GOT will test other critical distributed systems throughout 2004, including those systems residing on Windows and Unix-based platforms.

Why Test?

The main purpose of these exercises is not to simply test for the sake of testing, but to improve the accuracy of the disaster recovery plan and provide invaluable recovery experience to the team members. Being prepared for any situation that may affect an organization's ability to deliver critical services is a wise business decision. That is why GOT and multiple state agencies have committed a great deal of resources to develop their disaster recovery plans. The best way to determine if the plan is complete and effective is to conduct regular drills to test each facet of the plan. The test conducted in March accomplished the following:

—Restored the OS/390 mainframe environment for critical applications.
—Restored 33 critical mainframe applications to the hotsite mainframe.
—Tested backup-restore procedures.
—Tested communications to the hotsite.
—Tested agencies ability to enter transactions and verify processing capability.

Testing Results

GOT's disaster recovery plan for mainframe systems requires most mission critical systems to be operational within 48 hours of staff arriving at the recovery site. Cost is a major factor in determining the time period for applications and systems to be restored to operational status. In other words, the shorter the recovery timeframe, the more costly.

Some people have confused recovery time with recovery point. For example, the preceding section talked about the recovery time or time needed to restore data and applications so that processing can be resumed. Recovery point, on the other hand, is the point in time in which the data is restored. In the Commonwealth's case, the data was restored on Monday morning with the last full system backups that occurred on the previous weekend. An agency can then determine what course of action it needs to take to get to a current status depending upon when the disaster occurred. As a result of this year's testing, we have again found many areas that we can approve upon to ensure the timely recovery of critical systems. Next up: distributed applications!

Cyber Bytes

Current Security News & Information

Secure Your Network or Go to Jail

Organizations that do not make good faith efforts to secure their networks are likely to be held liable according to laws such as the 2002 Sarbanes-Oxley Act . The Sarbanes-Oxley Act requires company executives to pledge that their company's network infrastructure is secure. Many security and legal experts predict that due to the increasing focus on cyber terrorism more companies will be subject to criminal and civil penalties if they do not take efforts to adequately secure their systems. If you are interested in learning more about this issue, read the article at ZDNet.com.

New Bill to Outlaw Hidden Spyware

A new bill called 'The Software Principles Yielding Better Levels of Consumer Knowledge Act' or more simply known as the Spy Block Act has been introduced to the US Senate. The bill's purpose is to protect consumers from hidden spyware that is often times bundled in seemingly legitimate freeware or shareware and loaded unknowingly by users. The bill would make it illegal to install spyware on a computer without the user's knowledge and permission. For more information, read the article in Government Computer News.

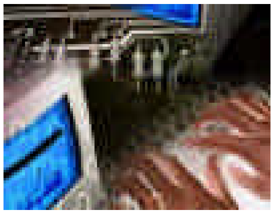
Damages from Mydoom, Netsky & Bagle Worms Surpass $100 Billion

According to mi2g Intelligence Unit, a digital risk firm, economic damages from the Mydoom, Netsky & Bagle worms have exceeded $100 billion, with the worms affecting computers in over 215 countries. All three worms also affected systems on the Kentucky Information Highway. More information can be found on Content Wire.

New Trend Seen in the Latest Worms

Symantec reports that it is seeing a new trend in worms that take advantage of specific vulnerabilities in the Microsoft Windows operating system, a mode of attack unheard of before 2003. Former worms like Nimda and Code Red targeted servers, not the operating system. More information on this new worm trend can be found in the Seattle Times Article.

New 'How To' Book for Malicious Code Writers



Security researchers have recently published a book that details how to write malicious code to exploit software vulnerabilities. The book entitled, The Shellcoder's Handbook: Discovering and Exploiting Security Holes, was written to be a resource for network administrators to use for closing security holes but seems to have shared some previously unknown info that may benefit malicious code writers and hackers. Looks like the researchers may have opened a whole new can of worms, pardon the pun. Read the article at NWFusion to learn more.

Microsoft Updates

Microsoft has released the following security updates for its operating systems and other software products. GOT recommends that agencies devise procedures to ensure the timely installation of hardware and software patches/updates, as well as the update of virus definition files. A comprehensive list of hardware and software security vulnerabilities affecting multiple platforms can be found on the GOT Security Alerts webpage.

Microsoft Security Bulletin MS04-008

Vulnerability in Windows Media Services Could Allow a Denial of Service (832359)

Affects Microsoft Windows 2000. A vulnerability exists because of the way that Windows Media Station Service and Windows Media Monitor Service, components of Windows Media Services, handle TCP/IP connections. If a remote user were to send a specially-crafted sequence of TCP/IP packets to the listening port of either of these services, the service could stop responding to requests and no additional connections could be made. The service must be restarted to regain its functionality.

Microsoft Security Bulletin MS04-009

Vulnerability in Microsoft Outlook Could Allow Code Execution (828040)

Affects Outlook 2002 and Office XP. A security vulnerability exists within Outlook 2002 that could allow Internet Explorer to execute script code in the Local Machine zone on an affected system.

Microsoft Security Bulletin MS04-010

Vulnerability in MSN Messenger Could Allow Information Disclosure (838512)

Affects MSN Messenger 6.0 & 6.1. A security vulnerability exists in Microsoft MSN Messenger due to the method used by MSN Messenger to handle a file request. An attacker could exploit this vulnerability by sending a specially crafted request to a user running MSN Messenger.

Upcoming Microsoft Webcast Offerings

Microsoft offers numerous free webcasts on security-related topics. To learn more about upcoming live webcasts, check out Microsoft's webpage. Please note that in order to view the webcasts, you must first install Microsoft's Live Meeting software. Check out this Microsoft FAQ for more information on installing Live Meeting.

Microsoft Security Site

Microsoft has developed a security page that contains the latest information on Microsoft security bulletins and virus alerts. The page features many 'how to' articles and tips to help identify the latest threats and help you to better protect your system. To learn more, go to http://www.microsoft.com/security/ on the web.

Microsoft Security Tools

Microsoft site that provides tools to assess vulnerabilities and strengthen security. To learn more, click here.

Automatically Update Your Computer

Windows Update allows you to automatically update your computer's operating system, software, and hardware with the latest security patches. To learn more, visit the Windows Update Site and follow the prompts.

GOVERNOR'S OFFICE FOR TECHNOLOGY

Division of Security Services
101 Cold Harbor Drive
Frankfort, KY 40601

Phone: 502-564-7680

Email:
GOTSecurityServices@ky.gov

We're on the Web!
ky.gov/got/security/

The information contained in this newsletter is intended for internal use only.

Division of Security Services — Keeping the Commonwealth's Computing Resources Secure

The Governor's Office for Technology's Security Awareness Newsletter is published bi-monthly by the Division of Security Services. Its purpose is to provide security & IT professionals with timely information on cyber vulnerabilities, information security trends, malicious code info, and security policies & practices.

About the Division of Security Services

The Division of Security Services' (DSS) primary role is to protect and ensure the confidentiality, integrity, and availability of the Commonwealth's computing environment, which includes the Kentucky Information Highway (KIH), Commonwealth Data Center (CDC), and other key state computing facilities.

Security Services is also responsible for the development and maintenance of GOT's Security Policies and Procedures Manual (SPPM), disaster recovery/business continuity plan, and Security Administrator Manuals (SAMs) that aid network administrators in securely configuring Windows NT, 2000, and Unix Solaris & AIX systems. DSS also provides mainframe RACF, computer forensics, and password auditing services to state agencies upon request. If you would like to learn more about the services that DSS provides, visit our web page.

For more information on IT Security, check out the following websites!

McAfee Virus Information—NAI's McAfee virus information site that contains the latest virus alerts and breaking news. Also contains links to virus removal tools, malicious code definitions and more.

NSA Information Assurance—The National Security Agency's site that provides information on detecting, reporting, and responding to cyber threats. Site also has links to security configuration guides to enhance the security of operating systems, routers, web browsers, and software applications.

HelpNet Security—Daily updated site that provides the latest advisories, viruses, press releases, and papers.

NIST Computer Security Resource Center—National Institute of Standards and Technology's site that contains information on various security-related topics such as cryptology, security testing, research, awareness and management.

Home Network Security—Site sponsored by the CERT Coordination Center that gives home users an overview of the security risks associated with home networks.

Windows Security—Website that provides the latest Windows security news, articles, FAQs, and tutorials.

ComputerWorld Security Site—IT-based magazine site that is an excellent resource for various topics related to information technology security.